

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 1 0 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 1 8 4 7 6
Application Number:

[ST. 10/C]: [J P 2 0 0 3 - 3 1 8 4 7 6]

出 願 人 株式会社リコー
Applicant(s):

2 0 0 3 年 1 0 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 0306411
【提出日】 平成15年 9月10日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G03G 21/00 370
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 大石 勉
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 平井 卓見
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 中川 克彦
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-269285
 【出願日】 平成14年 9月13日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

複数のアプリケーションを搭載可能に構成された画像形成装置であって、
一又は複数の認証手段からの認証結果を受信し、受信した認証結果に基づき、一又は複数のアプリケーションの利用制限を制御する利用制御手段を備えたことを特徴とする画像形成装置。

【請求項 2】

前記利用制御手段は、あるアプリケーションに対応する一又は複数の認証手段を示す情報を参照することにより、当該アプリケーションの利用に際して当該一又は複数の認証手段に認証処理を行わせ、認証結果を当該アプリケーションに通知する請求項 1 に記載の画像形成装置。

【請求項 3】

前記利用制御手段は、ある認証手段に対応する一又は複数のアプリケーションを示す情報を参照することにより、当該一又は複数のアプリケーションのうちのいずれかのアプリケーションの利用に際して当該認証手段による認証結果をそのアプリケーションに通知する請求項 1 に記載の画像形成装置。

【請求項 4】

前記利用制御手段は、前記アプリケーションの機能毎に利用制限を制御する手段を有する請求項 1 に記載の画像形成装置。

【請求項 5】

前記利用制御手段は、複数の認証手段による認証が全て成功した場合に、その旨の認証結果をアプリケーションに通知する請求項 1 に記載の画像形成装置。

【請求項 6】

前記利用制御手段は、あるアプリケーションに対し、複数の認証手段による認証のうち少なくとも 1 つの認証手段による認証が成功した場合に、その旨の認証結果を前記アプリケーションに通知する請求項 1 に記載の画像形成装置。

【請求項 7】

前記認証手段は、画像形成装置上で実行されるアプリケーション又は画像形成装置の外部に接続される装置である請求項 1 ないし 6 のうちいずれか 1 項に記載の画像形成装置。

【請求項 8】

前記認証手段は、利用者により入力される利用者認証情報と、予め登録されている利用者認証情報とにより認証を行う請求項 1 ないし 6 のうちいずれか 1 項に記載の画像形成装置。

【請求項 9】

前記認証手段は、利用者により入力される課金情報と、予め登録されている利用可能課金情報とにより認証を行う請求項 1 ないし 6 のうちいずれか 1 項に記載の画像形成装置。

【請求項 10】

前記画像形成装置は、画像形成処理で使用されるハードウェア資源と、当該ハードウェア資源の制御を含むシステム側の処理を行うコントロールサービスとを備え、当該コントロールサービスとは別に複数のアプリケーションを搭載可能に構成され、

前記画像形成装置は、前記利用制御手段を、前記コントロールサービスとして備えた請求項 1 ないし 9 のうちいずれか 1 項に記載の画像形成装置。

【請求項 11】

前記認証手段は、
利用者に利用者識別情報と利用者認証情報を入力させる利用者情報入力手段と、
ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力手段によって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信手段と、

前記外部サーバ通信手段によって受信した利用者認証情報と、前記利用者情報入力処理

手段によって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、前記利用制御手段に通知する手段と

を備えた請求項 1 に記載の画像形成装置。

【請求項 1 2】

前記認証手段は、

利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信手段と、

前記利用者情報受信手段によって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信手段と、

前記外部サーバ通信手段によって受信した課金情報と、前記利用者情報受信手段によって受信した課金情報とを比較し、前記利用制御手段に通知する課金処理手段と、

を備えた請求項 1 に記載の画像形成装置。

【請求項 1 3】

前記利用者情報受信手段は、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信する請求項 1 2 に記載の画像形成装置。

【請求項 1 4】

前記外部サーバは、ネットワーク上の L D A P サーバである請求項 1 1 ないし 1 3 のうちいずれか 1 項に記載の画像形成装置。

【請求項 1 5】

複数のアプリケーションを搭載可能に構成された画像形成装置におけるアプリケーションの利用制御方法であって、

一又は複数の認証手段からの認証結果を受信し、受信した認証結果に基づき、一又は複数のアプリケーションの利用制限を制御する利用制御ステップを有することを特徴とする利用制御方法。

【請求項 1 6】

前記利用制御ステップにおいて、前記画像形成装置は、あるアプリケーションに対応する一又は複数の認証手段を示す情報を参照することにより、当該アプリケーションの利用に際して当該一又は複数の認証手段に認証処理を行わせ、認証結果を当該アプリケーションに通知する請求項 1 5 に記載の利用制御方法。

【請求項 1 7】

前記利用制御ステップにおいて、前記画像形成装置は、ある認証手段に対応する一又は複数のアプリケーションを示す情報を参照することにより、当該一又は複数のアプリケーションのうちのいずれかのアプリケーションの利用に際して当該認証手段による認証結果をそのアプリケーションに通知する請求項 1 5 に記載の利用制御方法。

【請求項 1 8】

前記利用制御ステップにおいて、前記画像形成装置は、前記アプリケーションの機能毎に利用制限を制御する請求項 1 5 に記載の利用制御方法。

【請求項 1 9】

前記利用制御ステップにおいて、前記画像形成装置は、複数の認証手段による認証が全て成功した場合に、その旨の認証結果をアプリケーションに通知する請求項 1 5 に記載の利用制御方法。

【請求項 2 0】

前記利用制御ステップにおいて、前記画像形成装置は、あるアプリケーションに対し、複数の認証手段による認証のうち少なくとも 1 つの認証手段による認証が成功した場合に、その旨の認証結果を前記アプリケーションに通知する請求項 1 5 に記載の利用制御方法。

【請求項 2 1】

前記認証手段は、画像形成装置上で実行されるアプリケーション又は画像形成装置の外部に接続される装置である請求項 1 5 ないし 2 0 のうちいずれか 1 項に記載の利用制御方法。

【請求項 2 2】

前記認証手段は、利用者により入力される利用者認証情報と、予め登録されている利用者認証情報とにより認証を行う請求項 1 5 ないし 2 0 のうちいずれか 1 項に記載の利用制御方法。

【請求項 2 3】

前記認証手段は、利用者により入力される課金情報と、予め登録されている利用可能課金情報とにより認証を行う請求項 1 5 ないし 2 0 のうちいずれか 1 項に記載の利用制御方法。

【請求項 2 4】

前記画像形成装置は、画像形成処理で使用されるハードウェア資源と、当該ハードウェア資源の制御を含むシステム側の処理を行うコントロールサービスとを備え、当該コントロールサービスとは別に複数のアプリケーションを搭載可能に構成され、

前記利用制御ステップは、前記コントロールサービスにより実行される請求項 1 5 ないし 2 3 のうちいずれか 1 項に記載の利用制御方法。

【請求項 2 5】

前記認証手段は、利用者により利用者識別情報と利用者認証情報を入力させる利用者情報入力手段と、ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力手段によって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信手段と、

前記外部サーバ通信手段によって受信した利用者認証情報と、前記利用者情報入力処理手段によって入力された利用者認証情報とが一致するか否かを判断する手段とを備えた請求項 1 5 に記載の利用制御方法。

【請求項 2 6】

前記認証手段は、利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信手段と、

前記利用者情報受信手段によって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信手段と、

前記外部サーバ通信手段によって受信した課金情報と、前記利用者情報受信手段によって受信した課金情報とを比較する課金処理手段と、を備えた請求項 1 5 に記載の利用制御方法。

【請求項 2 7】

前記利用者情報受信手段は、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信する請求項 2 6 に記載の利用制御方法。

【請求項 2 8】

前記外部サーバは、ネットワーク上の L D A P サーバである請求項 2 5 ないし 2 7 のうちいずれか 1 項に記載の利用制御方法。

【書類名】明細書

【発明の名称】画像形成装置及び利用制御方法

【技術分野】

【0001】

この発明は、コピー、プリンタ、スキャナ、ファクシミリなどの画像形成処理にかかるユーザサービスを提供し、複数の認証／課金装置、認証／課金アプリ等を一括して管理することのできる画像形成装置に関するものである。

【背景技術】

【0002】

近年では、プリンタ、コピー、ファクシミリ、スキャナなどの各装置の機能を1つの筐体内に収納した画像形成装置（以下、「複合機」という。）が知られている。この複合機は、1つの筐体内に表示部、印刷部および撮像部などを設けるとともに、プリンタ、コピーおよびファクシミリ装置にそれぞれ対応した3種類のソフトウェアを設け、これらのソフトウェアを切り替えることによって、当該装置をプリンタ、コピー、スキャナ又はファクシミリ装置として動作させるものである。

【0003】

ところで、このような従来の複合機では、プリンタ、コピー、スキャナおよびファクシミリ装置に対応するソフトウェアをそれぞれ別個に設けているため、各ソフトウェアの開発に多大の時間を要する。このため、出願人は、表示部、印刷部および撮像部などの画像形成処理で使用されるハードウェア資源を有し、プリンタ、コピー又はファクシミリなどの各ユーザサービスにそれぞれ固有の処理を行うアプリケーションを複数搭載し、これらのアプリケーションとハードウェア資源との間に介在して、ユーザサービスを提供する際に、アプリケーションの少なくとも2つが共通的に必要とするハードウェア資源の管理、実行制御並びに画像形成処理を行う各種コントロールサービスからなるプラットフォームを含む画像形成装置（複合機）を発明した。

【0004】

このような複合機では、利用者が複合機を利用する際にユーザIDとパスワードなどによる利用者認証を行い、複合機の不正な利用者による利用を制限したり、利用者の課金情報に基づいて利用制限を行ってセキュリティ面の強化を図っているものがある。このような認証機能および課金機能を備えた複合機では、一般的に、ユーザIDとパスワードを自己の記憶装置内の認証データベースで管理し、ユーザIDと課金情報を自己の記憶装置内の課金データベースで管理することが一般的となっている。特に、近年、複合機の使用形態としては、LAN（Local Area Network）やインターネットなどのネットワークに複数の複合機あるいはプリンタ装置を接続し、ネットワーク上のPC（Personal Computer）やワークステーションなどのコンピュータから利用するというものが一般的となっている。このため、ネットワークに接続された複合機ごとに認証データベースや課金データベースを設け、各複合機を利用可能な利用者のユーザIDおよびパスワードを管理する必要がある。

【特許文献1】特開2002-149362号公報

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、このようなユーザIDやパスワードなどの認証情報や課金情報を、自己の複合機内の認証データベースあるいは課金データベースで管理する場合、ネットワークに接続された個々の複合機ごとに認証データベースおよび課金データベースを設けて、それぞれ別個に管理しなければならないため、認証情報や課金情報の管理が煩雑になるという問題がある。

【0006】

すなわち、ネットワーク上の個々の複合機について、各複合機ごとに利用可能な利用者と利用不可能な利用者が異なる場合が考えられるため、利用者の固有の情報や認証情報あ

るいは課金情報を更新する場合に、どの複合機で利用可能な利用者かを判断しなければならず、ネットワーク上に多数の複合機が接続されている場合には、認証情報や課金情報の管理労力が増大する。また、複合機のシステム管理者以外に認証情報の追加、変更、削除などの認証データベースの更新、あるいは課金データベースの更新が制限されている場合でも、一人の利用者の認証情報又は課金情報に変更がある場合、ネットワーク上のすべての複合機の認証データベースおよび課金データベースの更新が必要となるため、複合機ごとにシステム管理者が異なれば、認証情報や課金情報のメンテナンス作業の労力が膨大なものとなる。

【0007】

また、ネットワーク上の各複合機ごとに認証データベース、課金データベースを管理する場合には、認証データベースの更新を複合機のシステム管理者のみに制限している場合であっても、利用者のシステム管理者のなりすましによって、パスワードを変更するなどの認証データベースや課金データベースを不正に改ざんすることが容易に可能となってしまう、セキュリティ面の脆弱性が問題となる。

【0008】

更に、認証や課金の方法には複数の方法が存在し、複数の認証／課金システムが複合機で使用される可能性があるが、これらを一括して管理することにより、これらを一又は複数のアプリケーションの利用制限のために使用する技術は従来はなかった。

【0009】

この発明は上記に鑑みてなされたもので、利用者の認証情報や課金情報などの利用者情報を管理するネットワーク上の外部サーバを利用した認証／課金システムを含む複数の認証／課金システムを複数のアプリに対して使用することを可能とした画像形成装置を提供することを目的とする。

【課題を解決するための手段】

【0010】

上記の課題を解決するために、請求項1に記載の発明は、複数のアプリケーションを搭載可能に構成された画像形成装置であって、一又は複数の認証手段からの認証結果を受信し、受信した認証結果に基づき、一又は複数のアプリケーションの利用制限を制御する利用制御手段を備える。

【0011】

本発明によれば、一又は複数の認証手段を一又は複数のアプリケーションに対して適用することができる。

【0012】

請求項2に記載の発明は、請求項1の記載において、前記利用制御手段は、あるアプリケーションに対応する一又は複数の認証手段を示す情報を参照することにより、当該アプリケーションの利用に際して当該一又は複数の認証手段に認証処理を行わせ、認証結果を当該アプリケーションに通知する。

【0013】

本発明によれば、あるアプリケーションの利用に際して、予めそのアプリケーションに対して設定された一又は複数の認証手段の認証を行うことが可能となる。

【0014】

請求項3に記載の発明は、請求項1の記載において、前記利用制御手段は、ある認証手段に対応する一又は複数のアプリケーションを示す情報を参照することにより、当該一又は複数のアプリケーションのうちのいずれかのアプリケーションの利用に際して当該認証手段による認証結果をそのアプリケーションに通知する。

【0015】

本発明によれば、一又は複数のアプリケーションの利用に際して、予め設定された認証手段を用いて認証を行うことが可能となる。

【0016】

請求項4に記載の発明は、請求項1の記載において、前記利用制御手段は、前記アプリ

ケーションの機能毎に利用制限を制御する手段を有するものである。

【0017】

本発明によれば、アプリケーションの機能毎に、利用制限を制御することができる。

【0018】

請求項5に記載の発明は、請求項1の記載において、前記利用制御手段は、複数の認証手段による認証が全て成功した場合に、その旨の認証結果をアプリケーションに通知する。

【0019】

請求項6に記載の発明は、請求項1の記載において、前記利用制御手段は、あるアプリケーションに対し、複数の認証手段による認証のうち少なくとも1つの認証手段による認証が成功した場合に、その旨の認証結果を前記アプリケーションに通知する。

【0020】

請求項5、6の発明によれば、複数の認証手段間の関係を定めることができ、認証手段とアプリケーションの性質に応じた適切な認証を行うことが可能になる。

【0021】

請求項7に記載の発明は、請求項1ないし6のうちいずれか1項に記載の画像形成装置において、前記認証手段は、画像形成装置上で実行されるアプリケーション又は画像形成装置の外部に接続される装置であるとするものである。

【0022】

本発明によれば、認証手段として、新規の認証アプリケーションのみならず、既存の外部接続装置も使用できる。

【0023】

請求項8に記載の発明は、請求項1ないし6のうちいずれか1項に記載の画像形成装置において、前記認証手段は、利用者により入力される利用者認証情報と、予め登録されている利用者認証情報とにより認証を行うものである。

【0024】

本発明により、利用者認証情報による認証を行うことができる。利用者認証情報とは、ID、パスワードなどである。

【0025】

請求項9に記載の発明は、請求項1ないし6のうちいずれか1項に記載の画像形成装置において、前記認証手段は、利用者により入力される課金情報と、予め登録されている利用可能課金情報とにより認証を行うものである。本発明により、課金情報による認証を行うことができる。

【0026】

請求項10に記載の発明は、請求項1ないし9のうちいずれか1項に記載の画像形成装置において、前記画像形成装置は、画像形成処理で使用されるハードウェア資源と、当該ハードウェア資源の制御を含むシステム側の処理を行うコントロールサービスとを備え、当該コントロールサービスとは別に複数のアプリケーションを搭載可能に構成され、前記画像形成装置は、前記利用制御手段を、前記コントロールサービスとして備えたものである。

【0027】

また、請求項11に記載の発明は、請求項1の記載において、前記認証手段は、利用者に利用者識別情報と利用者認証情報を入力させる利用者情報入力手段と、ネットワークに接続され、前記利用者識別情報と前記利用者認証情報を管理する外部サーバに対し、前記利用者情報入力手段によって入力された利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された利用者認証情報を受信する外部サーバ通信手段と、前記外部サーバ通信手段によって受信した利用者認証情報と、前記利用者情報入力処理手段によって入力された利用者認証情報とが一致するか否かを判断し、判断結果を、前記利用制御手段に通知する手段とを備えたものである。

【0028】

本発明によれば、認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減することができる。また、画像形成装置のセキュリティの強化を図ることができる。

【0029】

請求項12に記載の発明は、請求項1の記載において、前記認証手段は、利用者識別情報と、利用者による画像形成装置の使用状況を示す課金情報とを、ネットワークに接続されたクライアント端末から受信する利用者情報受信手段と、前記利用者情報受信手段によって前記利用者識別情報と前記課金情報を受信したときに、前記ネットワークに接続され、前記利用者識別情報と前記課金情報とを管理する外部サーバに対し、前記利用者識別情報を送信し、外部サーバによって前記利用者識別情報に基づいて検索された課金情報を受信する外部サーバ通信手段と、前記外部サーバ通信手段によって受信した課金情報と、前記利用者情報受信手段によって受信した課金情報とを比較し、前記利用制御手段に通知する課金処理手段と、を備えたものである。

【0030】

本発明によれば、外部サーバで利用者識別情報と課金情報とを一括管理するので、自己の画像形成装置内に課金データベースを保持する必要がなくなり、課金データベースのメンテナンス作業の労力を軽減することができる。また、画像形成装置のセキュリティの強化を図ることができる。

【0031】

請求項13に記載の発明は、請求項12の記載において、前記利用者情報受信手段は、前記クライアント端末が外部記憶媒体から読み出した前記利用者識別情報と前記課金情報を、前記クライアント端末から受信するものである。

【0032】

請求項14に記載の発明は、請求項11ないし13のうちいずれか1項に記載の画像形成装置において、前記外部サーバは、ネットワーク上のLDAPサーバであるとするものである。本発明によれば、各種情報の管理を効率的に行うことが可能となる。

【0033】

請求項15～28に記載の発明は、上記の画像形成装置に適した方法の発明であり、上記の画像形成装置の発明と同様の作用効果を奏する。

【発明の効果】

【0034】

本発明によれば、一又は複数の認証手段を一又は複数のアプリケーションに対して適用することができるようになる。また、あるアプリケーションの利用に際して、予めそのアプリケーションに対して設定された一又は複数の認証手段の認証を行うことが可能になり、一又は複数のアプリケーションの利用に際して、予め設定された認証手段を用いて認証を行うことが可能となる。

【発明を実施するための最良の形態】

【0035】

以下に添付図面を参照して、この発明にかかる画像形成装置、利用者認証方法および課金処理方法の好適な実施の形態を詳細に説明する。

【0036】

(実施の形態1)

図1は、この発明の実施の形態1である画像形成装置（以下、「複合機」という。）の主要構成および複合機を含むネットワーク構成を示す説明図である。実施の形態1にかかる複合機100は、オペレーションパネルにユーザ名、パスワードの入力画面を表示し、入力されたユーザ名でインターネット上の外部サーバにパスワードの問い合わせを行い、入力されたパスワードと外部サーバから取得したパスワードによって利用者認証を行って、利用者のアプリケーションの利用制限を行うものである。

【0037】

図1に示すように、本実施の形態にかかる複合機100は、インターネット170に接

続されており、インターネット170にはLDAPサーバ(Lightweight Directory Access Protocol)300が接続されている。ここで、複合機100、LDAPサーバ300間の通信プロトコルはTCP/IPを利用している。

【0038】

本実施の形態の複合機100において本発明の利用者認証方法を実現するための主要構成としては、図1に示すように、認証アプリ117、コピーアプリなどのアプリケーションと、OCS126、SCS122、CCS129などの後述するコントロールサービスと、汎用OSのデーモン(プロセス)として動作するinetd141およびhttpd142と、ネットワークコントローラ103と、オペレーションパネル150とを主に備えている。

【0039】

LDAPサーバ300は、X.500ベースのディレクトリサービスをインターネット向けに軽量化したプロトコルに従ってディレクトリサービスを提供するサーバである。LDAPサーバ300には、ユーザ名に対し、パスワード、メールアドレス、他利用者の個人情報に対応づけられて記憶されている。

【0040】

認証アプリ117は、LDAPサーバを利用して、ユーザ名とパスワードによって利用者認証処理を行うものである。認証アプリ117は、利用者情報入力処理部151と、外部サーバ通信部152と、認証部153とから構成される。

【0041】

利用者情報入力処理部151は、利用者に固有のユーザ名(利用者識別情報)と、利用者の正当性を示すパスワード(利用者認証情報)の要求を行うユーザ名、パスワード入力画面をオペレーションパネル150の操作表示部に表示し、ユーザ名、パスワードの入力を受け付けるものである。

【0042】

外部サーバ通信部152は、インターネット170上のLDAPサーバ300に対して、オペレーションパネル150の操作表示部から入力されたユーザIDをLDAPサーバに送信して、複合機100におけるユーザ名の利用者のパスワードを検索させ、検索結果としてのパスワードを受信するものである。

【0043】

認証部153は、LDAPサーバ300から受信したパスワードとオペレーションパネルの操作表示部から入力されたパスワードが一致しているか否かを判断し、その判断結果(一致、もしくは不一致)を、他のプロセスであるCCS129にプロセス間通信によって送信するものである。

【0044】

CCS(Certification Control Service)129は、利用者の利用者制限や利用者の課金処理を行うコントロールサービスである。本実施の形態の複合機100では、CCS129は、認証アプリ117の認証部153から利用者認証の判断結果を受信して、利用者の利用制限をするか否かをコピーアプリ112に送信するようになっている。なお、OCS126、SCS122などのコントロールサービスについては後述する。

【0045】

inetd141は、データの送受信要求を常時監視し、特定のプロトコルに対する接続要求を検出した場合に、それぞれのプロトコルを処理するサーバプログラムを起動するデーモンであり、通常のUNIX(登録商標)におけるinetdと同様の処理が行われる。実施の形態1の複合機100では、httpプロトコルおよびhttpsプロトコルによるデータの送受信のためのポートを常時監視して、かかるポートでの接続要求を検出した場合に、httpd142を起動する。

【0046】

httpd142は、httpプロトコルおよびhttpsプロトコルで送信されてく

るメッセージを受信するポート 80 番を常時監視しており、このポート 80 番でリクエストメッセージの受信を行うとともに、レスポンスメッセージの送信を行うものである。なお、リクエストメッセージおよびレスポンスメッセージの構造は、通常の http プロトコルにおける各メッセージの構造と同様であり、各メッセージには、html 形式で記述されたメッセージボディが含まれている。

【0047】

ネットワークコントローラ 103 は、http プロトコル、https プロトコルによる各種データの通信を行うものである。

【0048】

次に、本実施の形態にかかる複合機 100 の全体の機能的構成について説明する。図 2 は、実施の形態 1 の複合機 100 の全体構成を示すブロック図である。

【0049】

図 2 に示すように、複合機 100 は、白黒レーザプリンタ (B&W LP) 101 と、カラーレーザプリンタ (Color LP) 102 と、ネットワークコントローラ 103 と、スキャナ、ファクシミリ、メモリなどのハードウェアリソース 104 を有するとともに、プラットフォーム 120 と、アプリケーション 130 とから構成されるソフトウェア群 110 とを備えている。

【0050】

プラットフォーム 120 は、アプリケーションからの処理要求を解釈してハードウェア資源の獲得要求を発生させるコントロールサービスと、一又は複数のハードウェア資源の管理を行い、コントロールサービスからの獲得要求を調停するシステムリソースマネージャ (SRM) 123 と、汎用 OS 121 とを有する。

【0051】

コントロールサービスは、複数のサービスモジュールから形成され、SCS (システムコントロールサービス) 122 と、ECS (エンジンコントロールサービス) 124 と、MCS (メモリコントロールサービス) 125 と、OCS (オペレーションパネルコントロールサービス) 126 と、FCS (ファックスコントロールサービス) 127 と、NCS (ネットワークコントロールサービス) 128 と、CCS (認証コントロールサービス) 129 から構成される。このプラットフォーム 120 は、あらかじめ定義された関数により前記アプリケーション 130 から処理要求を受信可能とするアプリケーションプログラムインタフェース (API) を有する。

【0052】

汎用 OS 121 は、UNIX (登録商標) などの汎用オペレーティングシステムであり、プラットフォーム 120 並びにアプリケーション 130 の各ソフトウェアをそれぞれプロセスとして並列実行する。

【0053】

SRM 123 のプロセスは、SCS 122 とともにシステムの制御およびリソースの管理を行うものである。SRM 123 のプロセスは、スキャナ部やプリンタ部などのエンジン、メモリ、HDD ファイル、ホスト I/O (セントロ I/F、ネットワーク I/F (ネットワークコントローラ 103)、IEEE 1394 I/F、RS 232C I/F など) のハードウェア資源を利用する上位層からの要求にしたがって調停を行い、実行制御する。

【0054】

具体的には、この SRM 123 は、要求されたハードウェア資源が利用可能であるか (他の要求により利用されていないかどうか) を判断し、利用可能であれば要求されたハードウェア資源が利用可能である旨を上位層に伝える。また、SRM 123 は、上位層からの要求に対してハードウェア資源の利用スケジューリングを行い、要求内容 (例えば、プリンタエンジンにより紙搬送と作像動作、メモリ確保、ファイル生成など) を直接実施している。

【0055】

SCS122のプロセスは、アプリ管理、操作部制御、システム画面表示、LED表示、リソース管理、割り込みアプリ制御などを行う。

【0056】

ECS124のプロセスは、白黒レーザプリンタ (B&W LP) 101、カラーレーザプリンタ (Color LP) 102、スキャナ、ファクシミリなどからなるハードウェアリソース104のエンジンの制御を行う。

【0057】

MCS125のプロセスは、画像メモリの取得および解放、ハードディスク装置 (HDD) の利用、画像データの圧縮および伸張などを行う。

【0058】

FCS127のプロセスは、システムコントローラの各アプリ層からPSTN/ISDN網を利用したファクシミリ送受信、BKM (バックアップSRAM) で管理されている各種ファクシミリデータの登録/引用、ファクシミリ読みとり、ファクシミリ受信印刷、融合送受信を行うためのAPIを提供する。

【0059】

NCS128のプロセスは、ネットワークI/Oを必要とするアプリケーションに対して共通に利用できるサービスを提供するためのプロセスであり、ネットワーク側から各プロトコルによって受信したデータを各アプリケーションに振り分けたり、アプリケーションからデータをネットワーク側に送信する際の仲介を行う。

【0060】

OCS126のプロセスは、オペレータ (ユーザ) と本体制御間の情報伝達手段となるオペレーションパネル (操作パネル) 150の制御を行う。OCS126は、オペレーションパネルからキー押下 (又はタッチ操作) をキーイベントとして取得し、取得したキーに対応したキーイベント関数をSCS122に送信するOCSプロセスである。また、オペレーションパネル150の操作表示部に対する各種画面を描画出力やその他オペレーションパネルに対する制御は、OCS関数ライブラリに登録されている描画関数等の各種関数をアプリケーション130又はコントロールサービスから呼び出すことにより行われる。このOCS関数ライブラリは、アプリケーション130およびコントロールサービスの各モジュールに動的にリンクされている。なお、OCS126のすべてをプロセスとして動作させるように構成しても良く、あるいはOCS126のすべてをOCS関数ライブラリとして構成しても良い。

【0061】

アプリケーション130は、ページ記述言語 (PDL)、PCLおよびポストスクリプト (PS) を有するプリンタ用のアプリケーションであるプリンタアプリ111と、コピー用アプリケーションであるコピーアプリ112と、ファクシミリ用アプリケーションであるファックスアプリ113と、スキャナ用アプリケーションであるスキャナアプリ114と、ネットワークファイル用アプリケーションであるネットファイルアプリ115と、工程検査用アプリケーションである工程検査アプリ116と、上述した認証アプリ117とを有している。

【0062】

アプリケーション130の各プロセス、コントロールサービスの各プロセスは、関数呼び出しとその戻り値送信およびメッセージの送受信によってプロセス間通信を行いながら、コピー、プリンタ、スキャナ、ファクシミリなどの画像形成処理にかかるユーザサービスを実現している。

【0063】

このように、実施の形態1にかかる複合機100には、複数のアプリケーション130および複数のコントロールサービスが存在し、いずれもプロセスとして動作している。そして、これらの各プロセス内部には、一又は複数のスレッドが生成されて、スレッド単位の並列実行が行われる。そして、コントロールサービスがアプリケーション130に対し共通サービスを提供しており、このため、これらの多数のプロセスが並列動作、およびス

レッドの並列動作を行って互いにプロセス間通信を行って協調動作をしながら、コピー、プリンタ、スキャナ、ファクシミリなどの画像形成処理にかかるユーザサービスを提供するようになっている。

【0064】

また、複合機100には、複合機100の顧客、サードベンダなどの第三者がコントロールサービス層の上のアプリケーション層に外部アプリを開発して搭載することが可能となっている。認証アプリ117は、このような外部アプリとして開発されたものであっても良い。

【0065】

なお、実施の形態1にかかる複合機100では、複数のアプリケーション130のプロセスと複数のコントロールサービスのプロセスとが動作しているが、アプリケーション130とコントロールサービスのプロセスがそれぞれ単一の構成とすることも可能である。また、各アプリケーション130は、アプリケーションごとに追加又は削除することができる。

【0066】

図3に複合機100のハードウェア構成例を示す。

【0067】

複合機100は、コントローラ160と、オペレーションパネル175と、ファックスコントロールユニット(FCU)176と、プリンタ等の画像形成処理に特有のハードウェア資源であるエンジン部177とを含む。コントローラ160は、CPU161と、システムメモリ162と、ノースブリッジ(NB)163と、サウスブリッジ(SB)164と、ASIC166と、ローカルメモリ167と、HDD168と、ネットワークインターフェースカード(NIC)169と、SDカード用スロット170と、USBデバイス171と、IEEE1394デバイス172と、センタロニクス173とを含む。なお、メモリ162、167はRAM、ROM等を含む。FCU176およびエンジン部177は、コントローラ160のASIC166にPCIバス178で接続されている。

【0068】

CPU161が、複合機100にインストールされるアプリケーション、コントロールサービス等のプログラムを、メモリから読み出して実行する。

【0069】

次に、以上のように構成された実施の形態1にかかる複合機100による利用者認証方法について説明する。図4は、複合機100による利用者認証処理におけるデータの流れを示す説明図であり、図5は、利用者認証処理の手順を示すフローチャートである。

【0070】

本実施の形態の複合機100では、電源投入後、まずコピーアプリ112が優先的に起動し、その際に利用者認証が行われ、認証結果が正当であれば、コピーアプリ112が初期画面をオペレーションパネル150の操作表示部150aに出力し、コピー操作ができるようになっている。

【0071】

まず、認証アプリ117の利用者情報入力処理部151は、オペレーションパネル150の操作表示部150aに図6に示すユーザ名・パスワード入力画面501を表示する(ステップS401)。ここで各種画面の操作表示部150aへの表示は、OCS関数ライブラリの描画関数呼び出しによって行われる。以下、操作表示部150aへの表示の説明では、描画関数呼び出しを行うことを前提とし、その旨の説明は省略する。また、操作表示部150aからキー入力を行った場合、入力キーのキーイベントをOCS126で取得して、SCS122を経由して認証アプリ117の利用者情報入力処理部151に通知される。

【0072】

ユーザ名・パスワード入力画面501からユーザ名、パスワードが入力されたら、認証アプリ117の外部サーバ通信部152は、入力されたユーザ名およびエントリ検索要求

をLDAPサーバ300に送信することにより、LDAPサーバ300によってユーザ名のエントリの検索を実行させる（ステップS402）。外部サーバ通信部152によるユーザ名およびエントリ検索要求のLDAPサーバ300への送信は、inetd141がhttpd142を起動し、httpd142からネットワークコントローラ103を経由して行われる。また、検索結果は、ネットワークコントローラ103、httpd142を経由して外部サーバ通信部152に通知される。

【0073】

ここで、ステップS402における外部サーバ通信部152によるLDAPサーバ300に対するエントリ検索要求の処理について説明する。図7は、エントリ検索要求処理の手順を示すフローチャートである。

【0074】

外部サーバ通信部152は、まず検索フィルタに入力されたユーザIDを設定する（ステップS601）。具体的には、例えば「user ID=XXXXXXXXX」という設定を行う。

【0075】

次に、これからの操作で使用するセッションハンドルを取得するため、ldap_init（）関数を発行する（ステップS602）。セッションハンドルを取得したら、LDAPサーバ300に対する検索関数を実行する。具体的には、接続先LDAPサーバのIPアドレス、接続先ポート、接続権限パスワード、検索位置、ステップS601で設定した検索フィルタ、検索属性（パスワードを指定）をパラメタとして指定して、ldaps_eaarch（）関数を呼び出す（ステップS603）。

【0076】

これにより、LDAPサーバ300で指定されたユーザIDに対応するパスワードが検索され、検索結果として検索されたパスワードがLDAPサーバから受信される（ステップS604）。そして、最後に、セッションハンドルを解放するため、ldap_unbind（）関数を呼び出す（ステップS605）。これにより一連の検索要求処理が完了する。

【0077】

図5に戻り、次に、認証アプリ117の認証部153は、LDAPサーバ300から受信した検索結果としてのパスワードと、ユーザ名・パスワード入力画面501から入力されたパスワードを比較して一致しているか否かを判断する（ステップS403）。そして、一致している場合には、認証結果「一致」をCCS129に送信する（ステップS404）。一方、両パスワードが一致していない場合には、認証結果「不一致」をCCS129に送信する（ステップS405）。

【0078】

認証結果を受信したCCS129は、認証結果が「一致」か否かを判断する（ステップS406）。そして、「一致」である場合には、正当な利用者であると判断しコピーアプリ112の利用制限を行わない。この場合、CCS129は、コピーアプリ112に対し、初期画面の表示要求を行う（ステップS407）。初期画面の表示要求を受けたコピーアプリ112は、オペレーションパネル150の操作表示部150aに初期画面を表示する（ステップS408）。

【0079】

一方、「不一致」である場合には、CCS129は、オペレーションパネル150の操作表示部150aにコピーアプリの利用が制限される旨のエラーメッセージを表示する（ステップS409）。これによって、利用者認証および利用制限の処理が完了する。

【0080】

なお、上記の実施の形態において、入力パスワードと登録パスワードとの一致判断の処理をLDAPサーバで行うようにしてもよい。また、パスワード、ユーザIDはそれぞれ、オペレーションパネルから入力することに代えて、ネットワーク接続されたPCから入力するようにしてもよい。

【0081】

このように実施の形態1にかかる複合機100では、認証アプリ117の利用者情報入力処理部151によって、利用者に固有のユーザIDとパスワードを入力させ、外部サーバ通信部152によって、インターネット170に接続されたLDAPサーバ300に対し入力されたユーザIDを送信し、LDAPサーバ300によって検索されたパスワードを受信し、認証部153によって、外部サーバ通信部152によって受信したパスワードと、利用者情報入力処理部151によって入力されたパスワードとが一致するか否かを判断し、判断結果を、CCS129に通知しているので、自己の複合機内に認証データベースを保持する必要がなくなり、認証データベースのメンテナンス作業の労力を軽減することができる。また、各複合機100に認証データベースを保持する必要がないため、パスワードなどの情報の改ざんを防止することができ、複合機100のセキュリティの強化を図ることができる。

【0082】

(実施の形態2)

実施の形態1にかかる複合機100は、オペレーションパネルにユーザ名、パスワードの入力画面を表示し、入力されたユーザ名でインターネット上の外部サーバにパスワードの問い合わせを行うものであったが、この実施の形態2にかかる複合機700は、インターネット上のPC200からユーザ名と課金データを受信して外部サーバに課金データの問い合わせを行うものである。

【0083】

図8は、実施の形態2にかかる複合機700の主要構成および複合機を含むネットワーク構成を示す説明図である。図9は、実施の形態2の複合機700の全体の機能的構成を示すブロック図である。

【0084】

図8に示すように、本実施の形態にかかる複合機700も、インターネット170に接続されており、インターネット170にはLDAPサーバ(Lightweight Directory Access Protocol)300とクライアント端末としてのPC(Personal Computer)が接続されている。ここで、複合機100、LDAPサーバ300およびPC200間の通信プロトコルはTCP/IPを利用している。

【0085】

本実施の形態の複合機700において本発明の課金処理方法を実現するための主要構成としては、図8に示すように、課金アプリ717、コピーアプリなどのアプリケーションと、OCS126、SCS122、CCS129、NCS126などの後述するコントロールサービスと、汎用OSのデーモン(プロセス)として動作するinetd141およびhttpd142と、ネットワークコントローラ103と、オペレーションパネル150とを主に備えている。

【0086】

本実施の形態のLDAPサーバ300は、ユーザ名に対し、パスワード、メールアドレスの他、課金データが対応づけられて記憶されている。課金データとしては、予算(使用可能金額)、A4使用可能枚数、B5使用可能枚数などがある。

【0087】

本実施の形態のPC200には、ICカードのリード制御を行うICカードリーダ201が接続されている。このICカードリーダ201に、ユーザ名、課金データが記録されたICカードを読み込ませ、ユーザ名、課金データをPC200から複合機700に送信するようになっている。ICカードに記録されている課金データとしては、使用金額、A4使用枚数、B5使用枚数などである。

【0088】

複合機700における課金アプリ717は、LDAPサーバ300を利用して、ユーザ名と課金データによって課金処理を行うものである。課金アプリ717は、利用者情報受

信部 751 と、外部サーバ通信部 752 と、課金処理部 753 とから構成される。

【0089】

利用者情報受信部 751 は、ユーザ名（利用者識別情報）と、パスワードを IC カードから読みとった PC 200 から受信するものである。

【0090】

外部サーバ通信部 752 は、インターネット 170 上の LDAP サーバ 300 に対して、オペレーションパネル 150 の操作表示部から入力されたユーザ ID を LDAP サーバに送信して、複合機 100 におけるユーザ名の利用者の課金データを検索させ、検索結果としての課金データを受信するものである。

【0091】

課金処理部 753 は、LDAP サーバ 300 から受信した課金データと PC 200 から受信した課金データを比較して、利用者の課金データが使用可能な範囲内か否かを判断し、その判断結果（範囲内、もしくは範囲外）を、他のプロセスである CCS 129 にプロセス間通信によって送信するものである。

【0092】

CCS (Certification Control Service) 129 は、利用者の利用者制限や利用者の課金処理を行うコントロールサービスである。本実施の形態の複合機 700 では、CCS 129 は、課金アプリ 717 の課金処理部 753 から課金処理の判断結果を受信して、利用者の利用制限をするか否かをコピーアプリ 112 に送信するようになっている。複合機 700 のその他の構成については、実施の形態 1 の複合機 100 と同様である。

【0093】

次に、以上のように構成された実施の形態 2 にかかる複合機 700 による課金処理および課金に基づく利用制限処理について説明する。図 10 は、複合機 700 による課金処理および課金に基づく利用制限処理におけるデータの流れを示す説明図であり、図 11 は、課金処理および課金に基づく利用制限処理の手順を示すフローチャートである。

【0094】

本実施の形態の複合機 700 では、インターネット 170 上の PC 200 からユーザ名、課金データを受信したときに、イベントドリブンで課金アプリ 717 が実行されるようになっている。そして、課金処理が行われ処理結果が正当であれば、コピーアプリ 112 が初期画面をオペレーションパネル 150 の操作表示部 150a に出力し、コピー操作ができるようになっている。

【0095】

課金アプリ 717 は、その利用者情報受信部 751 によって PC 200 からユーザ名、課金データを受信する。より具体的には、PC 200 によって送信されたユーザ名および課金データは、複合機 700 のネットワークコントローラ 104 で受信され、NCS 126 を経由して利用者情報受信部 751 で受信する。そして、外部サーバ通信部 752 は、受信したユーザ名およびエントリ検索要求を LDAP サーバ 300 に送信することにより、LDAP サーバ 300 によってユーザ名のエントリの検索を実行させる（ステップ S1001）。外部サーバ通信部 752 による LDAP サーバ 300 に対するエントリ検索要求の処理については、実施の形態 1 の複合機 100 と同様である。ただし、検索属性としては「課金データ」を設定して、ldapsearch 関数を呼び出すものとする。

【0096】

次に、課金アプリ 717 の課金処理部 753 は、LDAP サーバ 300 から受信した検索結果としての課金データと、PC 200 から受信した課金データを比較して、PC 200 から受信した課金データが複合機 700 の利用可能な範囲内か否かを判断する（ステップ S1002）。そして、範囲内である場合には、処理結果「範囲内」を CCS 129 に送信する（ステップ S1003）。一方、範囲外である場合には、処理結果「範囲外」を CCS 129 に送信する（ステップ S1004）。

【0097】

処理結果を受信したCCS129は、処理結果が「範囲内」か否かを判断する（ステップS1005）。例えば、使用金額が予算未満か否か、用紙の使用枚数が使用枚数未満か否かを判断する。そして、「範囲内」である場合には、利用者は複合機700をまだ使用できると判断しコピーアプリ112の利用制限を行わない。この場合、CCS129は、コピーアプリ112に対し、初期画面の表示要求を行う（ステップS1006）。初期画面の表示要求を受けたコピーアプリ112は、オペレーションパネル150の操作表示部150aに初期画面を表示する（ステップS1007）。

【0098】

一方、ステップS1005において、「範囲外」と判断された場合には、CCS129は、オペレーションパネル150の操作表示部150aにコピーアプリ112の利用が制限される旨のエラーメッセージを表示する（ステップS1008）。これによって、利用制限の処理が完了する。なお、認証結果を受けて、アプリ自身がエラーメッセージを表示するように構成してもよい。

【0099】

このように実施の形態2にかかる複合機700では、認証アプリ717の利用者情報受信部751によって、インターネット170上のPC200からユーザIDと課金データを受信し、外部サーバ通信部752によって、インターネット170に接続されたLDAPサーバ300に対し入力されたユーザIDを送信し、LDAPサーバ300によって検索された課金データを受信し、課金処理部753によって、外部サーバ通信部152によって受信した課金データと、利用者情報受信部751によって受信した課金データとを比較し、その比較結果を、CCS129に通知しているので、自己の複合機内に課金データベースを保持する必要がなくなり、課金データベースのメンテナンス作業の労力を軽減することができる。また、各複合機700に課金データベースを保持する必要がないため、課金データなどの情報の改ざんを防止することができ、複合機700のセキュリティの強化を図ることができる。

【0100】

なお、コピーを行う場合の課金処理は、例えば、次のようにして行うことができる。なお、以下の例では、LDAPサーバから受信した課金情報が、ユーザが利用可能なコピー枚数であり、ICカードから読み取った課金情報が既にユーザが使用した使用コピー枚数であるとする。

【0101】

上述の通り、既に使用した枚数が利用可能枚数より少なければユーザはコピーをすることができる。この場合、課金アプリは、利用可能枚数と使用枚数を保持する。そして、ユーザが原稿のコピーをする度に、コピーアプリは、SCS経由でECSに対して印刷ジョブを発行し、ECSからは排紙完了通知が課金アプリに対して通知される。排紙完了通知を受信すると、課金アプリは使用枚数に1加算し、加算した数と利用可能枚数とを比較する。また、ICカードにおける使用枚数を更新する。使用枚数が利用可能枚数より少なければコピーを継続できるが、使用枚数が利用可能枚数に達した場合には、課金アプリはCCSにその旨を通知し、CCSがコピーアプリに対して印刷中止の通知を行う。なお、上記の課金アプリは、所定の条件に基づき、ユーザによるアプリの使用の許可、非許可を決定するものであるので、認証アプリと称することもできる。

【0102】

（実施の形態3）

次に、実施の形態3について説明する。実施の形態1、2においては、認証アプリもしくは課金アプリのいずれかをを用いて利用者制限を行っていたが、実施の形態3に係る複合機は、複数の認証／課金のためのアプリもしくは装置を使用することを可能にするものである。

【0103】

実施の形態3における複合機の全体構成は図2に示すものとほぼ同様であるが、第3の実施の形態の複合機では、複数の認証／課金アプリを搭載し得る。また、第3の実施の形

態の複合機には、キーカウンタ、コインラック、キーカードなどの従来からある外部認証／課金装置を接続して使用することが可能である。

【0104】

図12は、第3の実施の形態におけるCCS129の機能の概要を説明するための図である。なお、以下の説明において、キーカウンタ、キーカード、コインラックのような外部接続認証／課金装置、及び、実施の形態1、2で説明したような認証／課金アプリにより認証／課金を行うシステムの両方を含む意味で「認証／課金システム」の用語を用いる。

【0105】

図12に示すように、CCS129は、複数の認証／課金システム、及び、認証／課金の対象となる複数のアプリを接続し、どのアプリに対してどの認証／課金システムを作用させるかを示す情報を管理する。複数の認証／課金システムの中には、既存のコインラックのような外部認証装置とともに、実施の形態1、2で説明したようなLDAPサーバを用いた認証／課金アプリを含む。例えば、認証／課金システム1は、複合機の搭載された新規の認証／課金アプリであり、認証／課金システム2は従来からあるキーカウンタやキーカードとする構成とすることができる。

【0106】

図13にCCS129のソフトウェア構成例を示す。実施の形態3におけるCCS129は、主制御部1291、ユーザコード部1292、キーカウンタ部1293、外部認証／課金システム部1294、拡張認証／課金システム部1295、及びデバイスインタフェース部1296を有している。

【0107】

主制御部1291がCCS129の全体の処理を実行するものである。ユーザコード部1292は、認証アプリもしくはSCS等によりユーザIDによるユーザ認証を行うためのものであり、どのアプリに対してユーザIDによるユーザ認証を行うかなどの設定情報を管理するとともに、認証結果の取得、認証結果の主制御部1291への通知等を行う。キーカウンタ部1293は、キーカウンタで認証／課金をおこなうためのものである。外部認証／課金システム部1294は、キーカードやコインラック等の外部認証／課金装置での認証／課金を行うためのものである。拡張認証／課金システム部1295は、実施の形態1、2で説明したようなLDAPサーバなどを用いた認証／課金システムにより認証／課金を行うためのものである。これらについても、ユーザコード部1292の場合と同様に、どのアプリに対して認証／課金を行うかなどの設定情報を管理するとともに、認証結果の取得、認証結果の主制御部1291への通知等を行う。なお、どのアプリに対してどの認証／課金を行うかの情報は、主制御部1291が参照するようにしてもよい。

【0108】

図13に示したCCS129は一例であり、接続する認証／課金装置、使用する認証／課金アプリに応じて、より多くの認証／課金システム部を設けることができる。

【0109】

デバイスインタフェース部1296は、キーカードやコインラック等の外部認証／課金装置とCCS129との接続のためのものである。例えば、図14に示すコードにより、キーカード装置等の外部接続装置にカードが挿入されたことを検知して、認証結果情報を読み取り、主制御部1291に、所定の処理をするように指示をする。所定の処理としては、例えば全てのアプリに、認証がOKなので動作を許可する指示をする処理がある。

【0110】

次に、認証／課金システムと、認証／課金の対象となるアプリとを対応付ける設定について説明する。この設定により、どのアプリがどの認証／課金システムを用いるかといった設定を行うことができる。

【0111】

図15～図18は、複合機のオペレーションパネルに表示される設定画面の例を示す図である。これらの画面は、CCS129が表示してもよいし、SCS122とCCS12

9との間で表示のための情報をやり取りすることによりSCS122が表示してもよい。以下、CCS129が表示を行うものとして説明する。

【0112】

まず、図15に示すように、使用できる認証／課金システムの一覧が表示される。ここで、「外部課金装置管理」は、コインラックやキーカード等の装置のための設定を行うためのボタンであり、「拡張認証／課金システム1管理」は、新規な認証／課金アプリのための設定を行うためのボタンである。なお、「次へ」のボタンを押すことにより、他の「拡張認証／課金システム2管理」などを表示させることができる。

【0113】

図15の画面において、「拡張認証／課金システム1管理」を選択すると、図16に示す画面が表示される。また、次項を押すことにより、図17に示すように、更に別の新規アプリも表示される。図16、図17に示す画面において、選択された拡張認証／課金システム1を用いて認証／課金を行う対象となるアプリを選択する。図16、図17に示す画面の例では、アプリの中のどの機能を対象にするかを選択することが可能である。例えば、コピーアプリの欄で「フルカラー」を選択した場合には、フルカラーのコピーを使用するときのみ、拡張認証／課金システム1による認証／課金動作が実施されることになる。

【0114】

このように設定された設定情報は、例えば、図18に示すような情報として記憶装置に記憶される。図18の設定では、アプリ1に対してはカラーの機能を使うときのみ拡張認証／課金システム1による利用制限処理がなされ、アプリ2に対しては全ての機能に対して利用制限処理がなされることを示している。

【0115】

そして、アプリ1の使用の際に、例えば、そのアプリ1においてカラーを用いようとしているとの情報がアプリ1からCCS129に通知され、CCS129はそのアプリ1の機能に対して、いずれかの認証／課金システムにて認証／課金を行うことの設定がなされているかを、図18に示す情報を参照して把握する。そして、該当の拡張認証／課金システムに対して動作するように指示を行う。

【0116】

なお、複数の認証／課金システムに対して、図16、17で示した画面で設定を行う場合、例えば、アプリ1の機能1に対して認証／課金システム1を動作させることの設定が既になされていて、更に、アプリ1の機能1に対して認証／課金システム2を動作させることの設定を行う場合には、後者の設定時に、前者との関係を入力させる画面を表示し、その関係を入力するようにしてもよい。例えば、認証／課金システム1と認証／課金システム2のうちのいずれかの認証が成功した場合にアプリ1の機能1の使用を許容する設定や、認証／課金システム1と認証／課金システム2の両方の認証が成功した場合にのみアプリ1の機能1の使用を許容する設定をすることができる。

【0117】

なお、図16～図18に示す画面の他に、図19～図20に示す画面を表示することも可能である。この場合には、例えば、図15の画面で拡張認証／課金システム1を選択した場合に、図19に示す画面が表示される。この画面で、アプリの機能を選択して設定を行うか、もしくは、アプリを選択して設定を行うかを選択する。

【0118】

アプリの機能を選択して設定を行うことを選択した場合、図16、図17と同様の画面が表示され、図16、図17と同様の設定を行うことができる。

【0119】

アプリを選択して設定を行うことを選択した場合には、図20の画面が表示される。ここで、あるアプリを選択した場合には、そのアプリのどの機能に対しても、該当の認証／課金アプリが動作する。図20に示す設定の場合には、例えば、図21に示す情報が記録され、CCS129が、この表を参照することにより、所定の認証／課金アプリを、使用

しようとするアプリに対して動作させる。例えば、コピー、アプリ 1 のうちのいずれかのアプリが利用されるに際して、認証／課金システム 1 が動作し、認証が行われ、CCS 経由で認証結果が当該利用しようとしているアプリに通知される。

【0120】

上記の例はある認証／課金システムに対して一つ又は複数のアプリを選択する例であったが、あるアプリに対して、そのアプリに適用する一つ又は複数の認証／課金システムを選択する設定を行うこともできる。そのような設定を行う場合の画面の例を図 22～図 23 に示す。

【0121】

まず、最初に図 22 の画面が表示される。この画面で、例えばアプリ 1 を選択すると、図 23 の画面が表示される。この画面で選択した認証／課金システムが、アプリ 1 に対して適用される。更に、複数の認証／課金システムを選択し、それらの全ての結果が OK であれば認証が OK であることをアプリに通知する AND 設定をすることもできるし、いずれかの結果が OK であれば認証が OK であることをアプリに通知する OR 設定を行うこともできる。この場合には、例えば、ある認証／課金システムを選択した後に、AND もしくは OR のボタンを押し、その後に、更に認証／課金システムを選択することにより、先に選択した認証システムと、後に選択した認証システムとで AND もしくは OR の関係を設定できる。この場合には、例えば「認証システム 1 AND 認証システム 2」なる情報が、該当のアプリに対応付けて記録される。そして、CCS 129 がこの情報を参照することにより、該当のアプリに対して、両方の認証／課金システムを動作させ、両方の認証／課金システムからの認証結果が OK であるときにのみ、認証 OK であることを該当のアプリに通知する。そして、アプリは動作可能な状態になる。

【0122】

なお、アプリの仕様によっては、使用できる認証／課金システムと使用できない認証／課金システムが存在し得るので、図 23 の画面を表示する前に、アプリから CCS 129 に対して、当該アプリに対応する認証／課金システムを知らせ、その情報を元に、CCS 129 が、アプリに適用できる認証／課金システムのみを図 23 の画面に表示してもよい。

【0123】

各認証／課金システムが動作する場合の CCS 129 の動作については、実施の形態 1、2 の場合と同様であるが、実施の形態 3 では、複数の認証／課金システムの結果を受信し、それらの全ての認証結果が OK である場合、もしくは、いずれか 1 つの認証結果が OK である場合に認証 OK であることを、設定情報を参照することにより、一つ又は複数のアプリに通知することができる。認証／課金アプリが動作する契機については、実施の形態 1 のように、電源投入時に起動されるアプリに対して認証画面を表示するようにしてもよいし、アプリ切り替えを CCS 129 が検出して、CCS 129 が、切り替えられたアプリに対応する認証／課金アプリに対して認証画面を表示するよう要求することもできる。なお、複数の認証／課金アプリが AND の関係にある場合には、例えば、それらの認証／課金アプリによる認証を順番に行うようにする。

【0124】

なお、本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【図面の簡単な説明】

【0125】

【図 1】実施の形態 1 にかかる複合機の主要構成および複合機を含むネットワーク構成を示す説明図である。

【図 2】実施の形態 1 の複合機の全体構成を示すブロック図である。

【図 3】実施の形態 1 の複合機のハードウェア構成を示すブロック図である。

【図 4】複合機による利用者認証処理におけるデータの流れを示す説明図である。

【図 5】利用者認証処理の手順を示すフローチャートである。

【図6】 ユーザ名・パスワード入力画面を示す説明図である。

【図7】 エントリ検索要求処理の手順を示すフローチャートである。

【図8】 実施の形態2にかかる複合機の主要構成および複合機を含むネットワーク構成を示す説明図である。

【図9】 実施の形態2の複合機の全体の機能的構成を示すブロック図である。

【図10】 複合機による課金処理および課金に基づく利用制限処理におけるデータの流れを示す説明図である。

【図11】 課金処理および課金に基づく利用制限処理の手順を示すフローチャートである。

【図12】 実施の形態3におけるCCSの機能を説明するための図である。

【図13】 CCSの機能的構成例を示す図である。

【図14】 デバイスインタフェース部による処理の一例を説明するための図である。

【図15】 CCSによる設定画面において、認証／課金システムの一覧表示がなされている画面の例である。

【図16】 認証／課金の対象とするアプリの機能を選択するための画面である。

【図17】 認証／課金の対象とするアプリの機能を選択するための画面である。

【図18】 図16、17の画面を用いた設定により格納される設定情報の例を示す図である。

【図19】 設定画面の他の例を示す図である。

【図20】 認証／課金の対象とするアプリを選択するための画面である。

【図21】 図20の画面を用いた設定により格納される設定情報の例を示す図である。

。

【図22】 設定画面の他の例を示す図である。

【図23】 アプリに対して適用する認証／課金システムを選択するための図である。

【符号の説明】

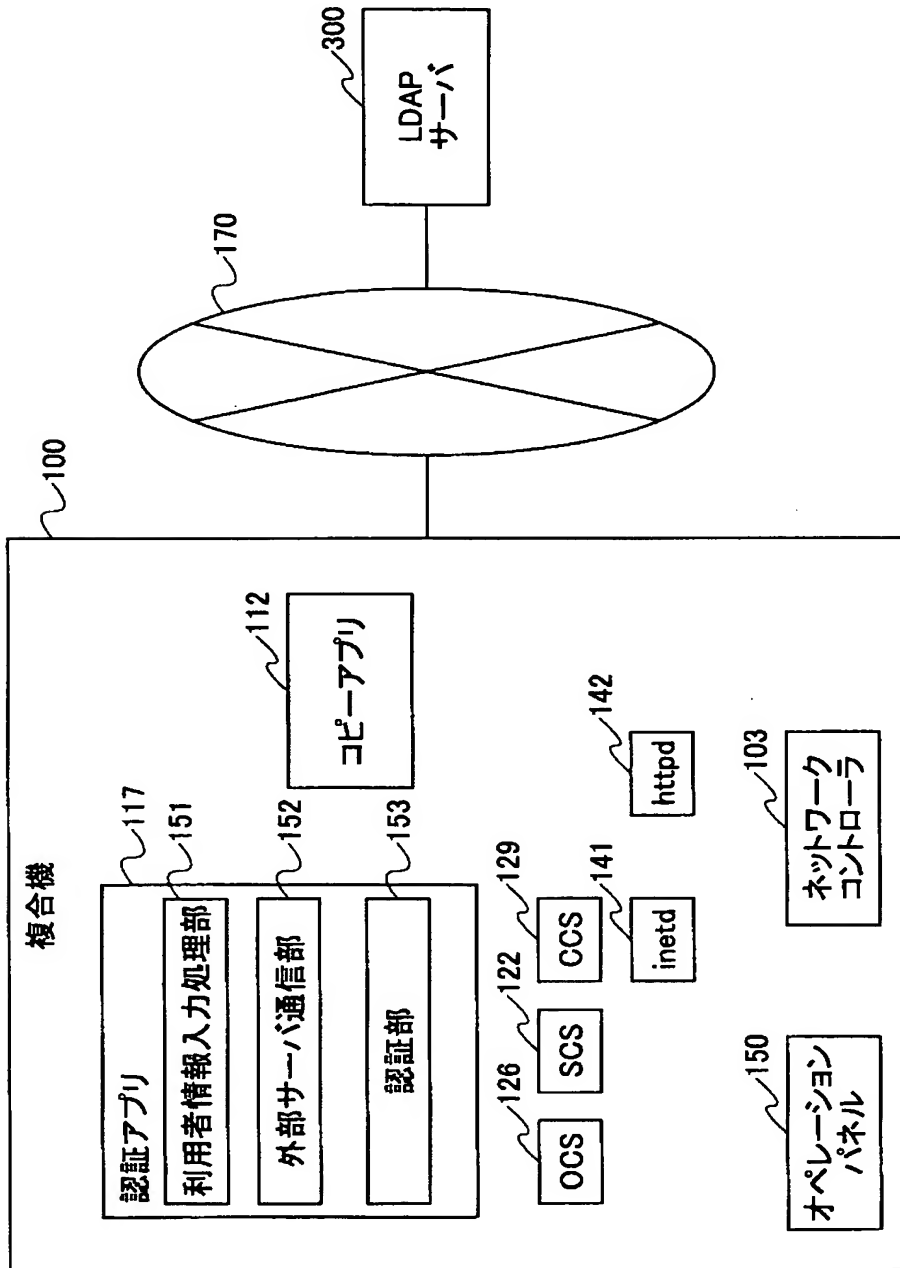
【0126】

- 100, 700 複合機
- 101 白黒レーザプリンタ
- 102 カラーレーザプリンタ
- 103 ネットワークコントローラ
- 104 ハードウェアリソース
- 110 ソフトウェア群
- 111 プリンタアプリ
- 112 コピーアプリ
- 113 ファックスアプリ
- 114 スキャナアプリ
- 115 ネットファイルアプリ
- 116 工程検査アプリ
- 117 認証アプリ
- 717 課金アプリ
- 120 プラットホーム
- 121 汎用OS
- 122 SCS
- 123 SRM
- 124 ECS
- 125 MCS
- 126 OCS
- 127 FCS
- 128 NCS
- 129 CCS

1 3 0 アプリケーション
 1 5 0 オペレーションパネル
 1 5 0 a 操作表示部
 1 5 1 利用情報入力処理部
 1 5 2, 7 5 2 外部サーバ通信部
 1 5 3 認証部
 1 7 0 インターネット
 2 0 0 P C
 2 0 1 I C カードリーダー
 3 0 0 L D A P サーバ
 5 0 1 ユーザ I D / パスワード入力画面
 7 5 1 利用情報受信部
 7 5 3 課金処理部
 1 2 9 1 主制御部
 1 2 9 2 ユーザコード部
 1 2 9 3 キーカウンタ部
 1 2 9 4 外部認証／課金システム部
 1 2 9 5 拡張認証／課金システム部

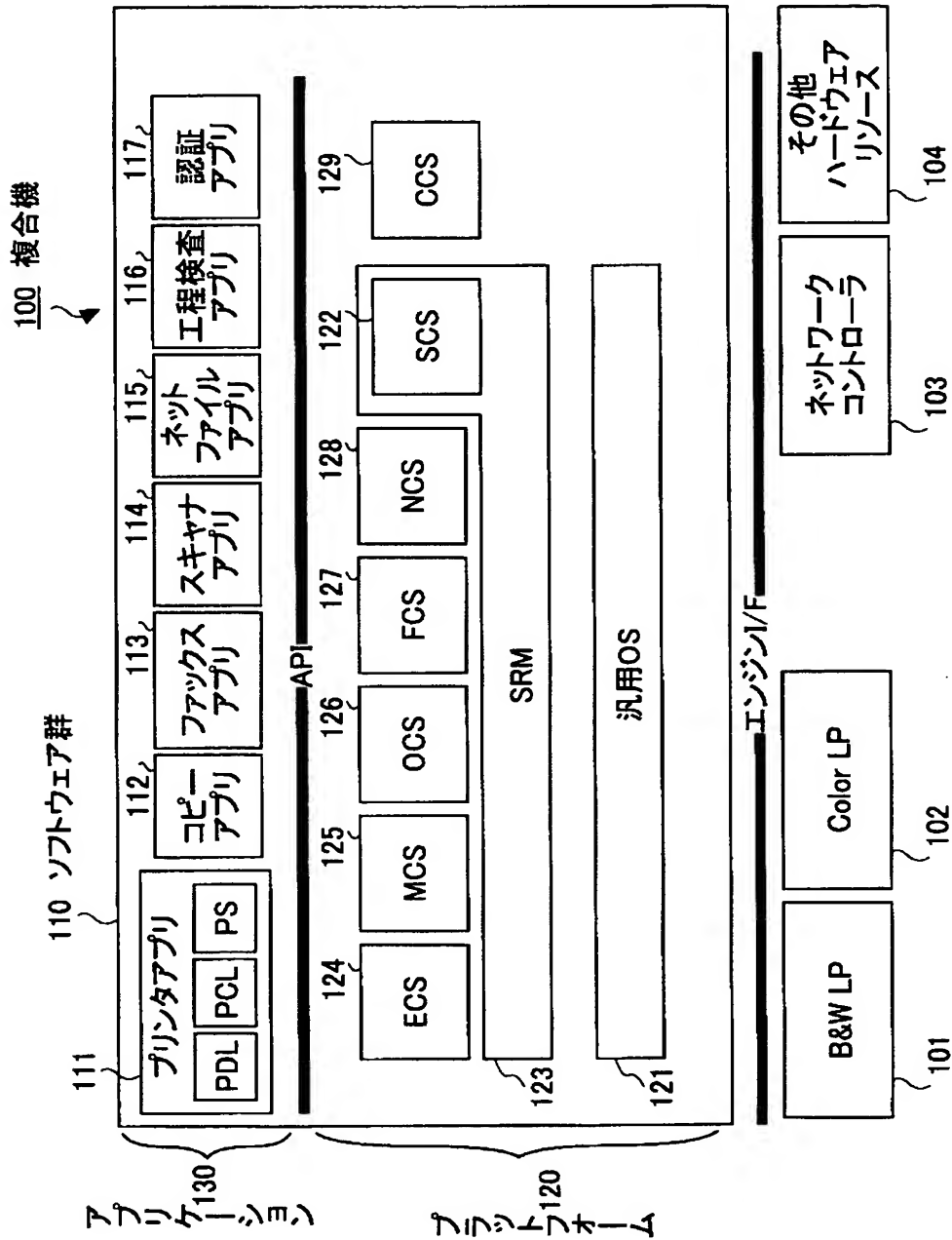
【書類名】 図面
【図 1】

実施の形態1にかかる複合機の主要構成および
複合機を含むネットワーク構成を示す説明図



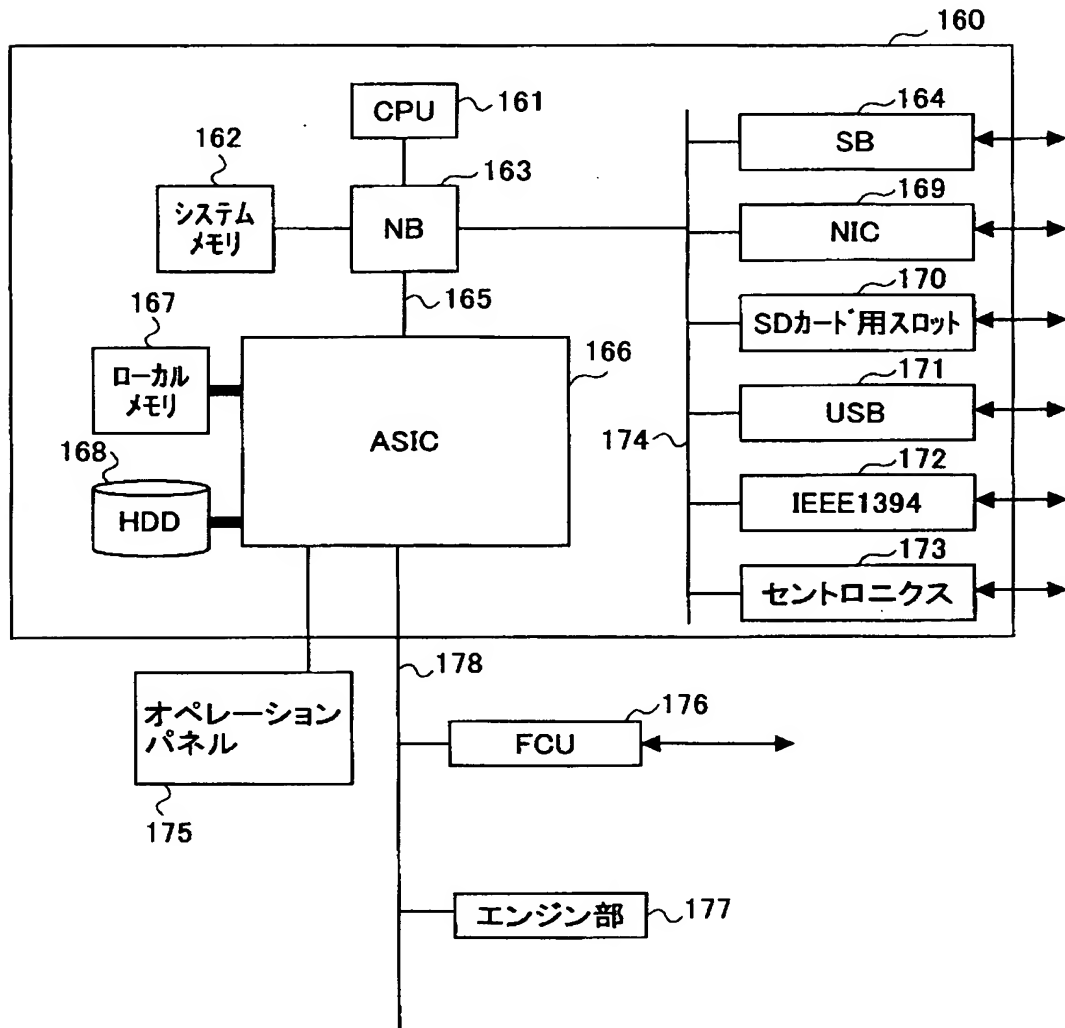
【図 2】

実施の形態1の複合機の全体構成を示すブロック図



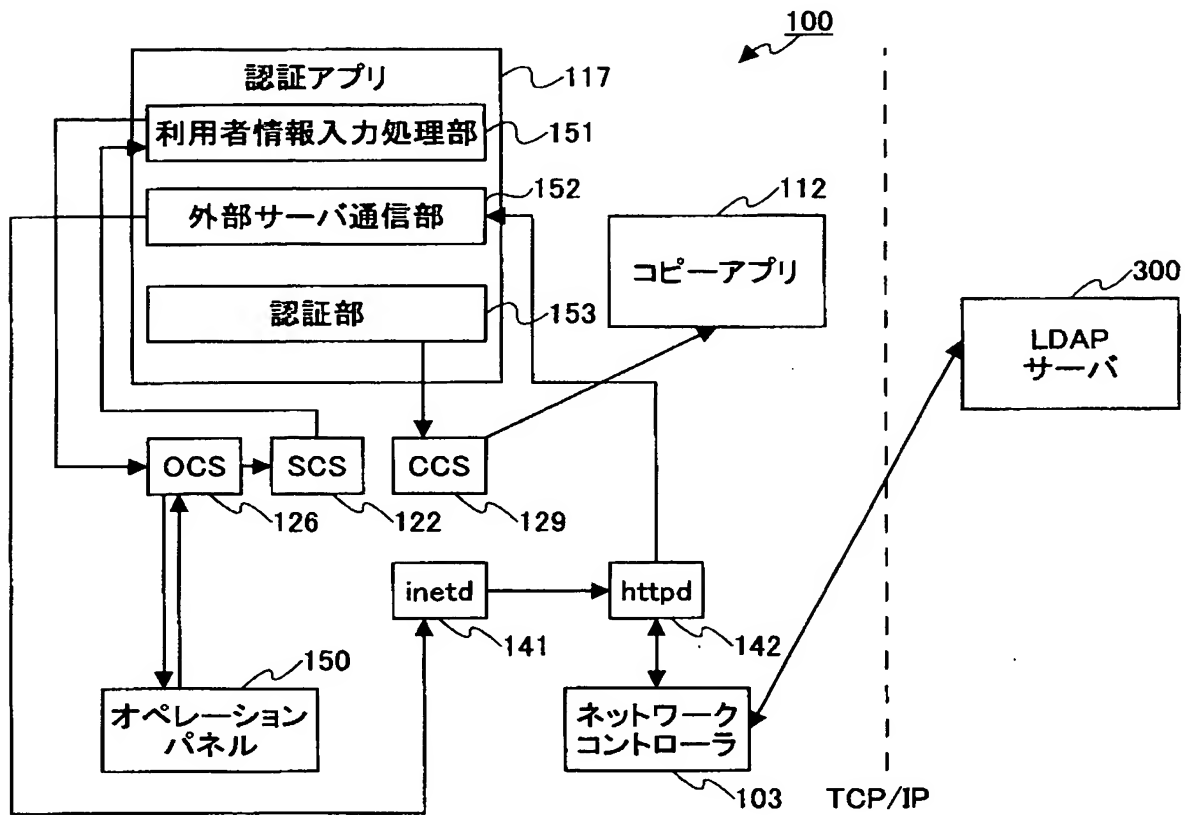
【図 3】

実施の形態 1 の複合機のハードウェア構成を示すブロック図



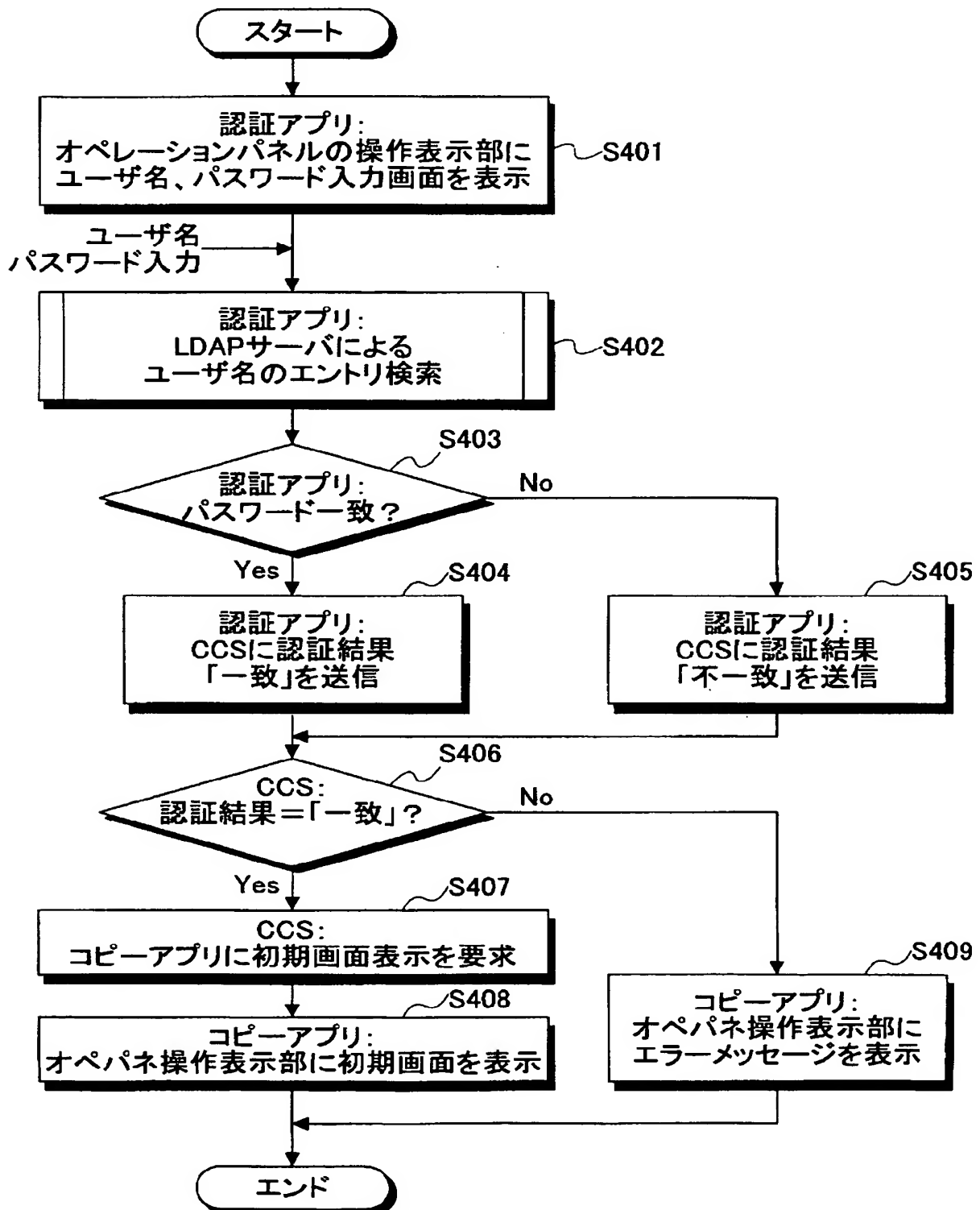
【図 4】

複合機による利用者認証処理におけるデータの流を示す説明図



【図 5】

利用者認証処理の手順を示すフローチャート



【図 6】

ユーザ名・パスワード入力画面を示す説明図

105a

ユーザ名・パスワード入力

ユーザID:

パスワード:

OK キャンセル

501

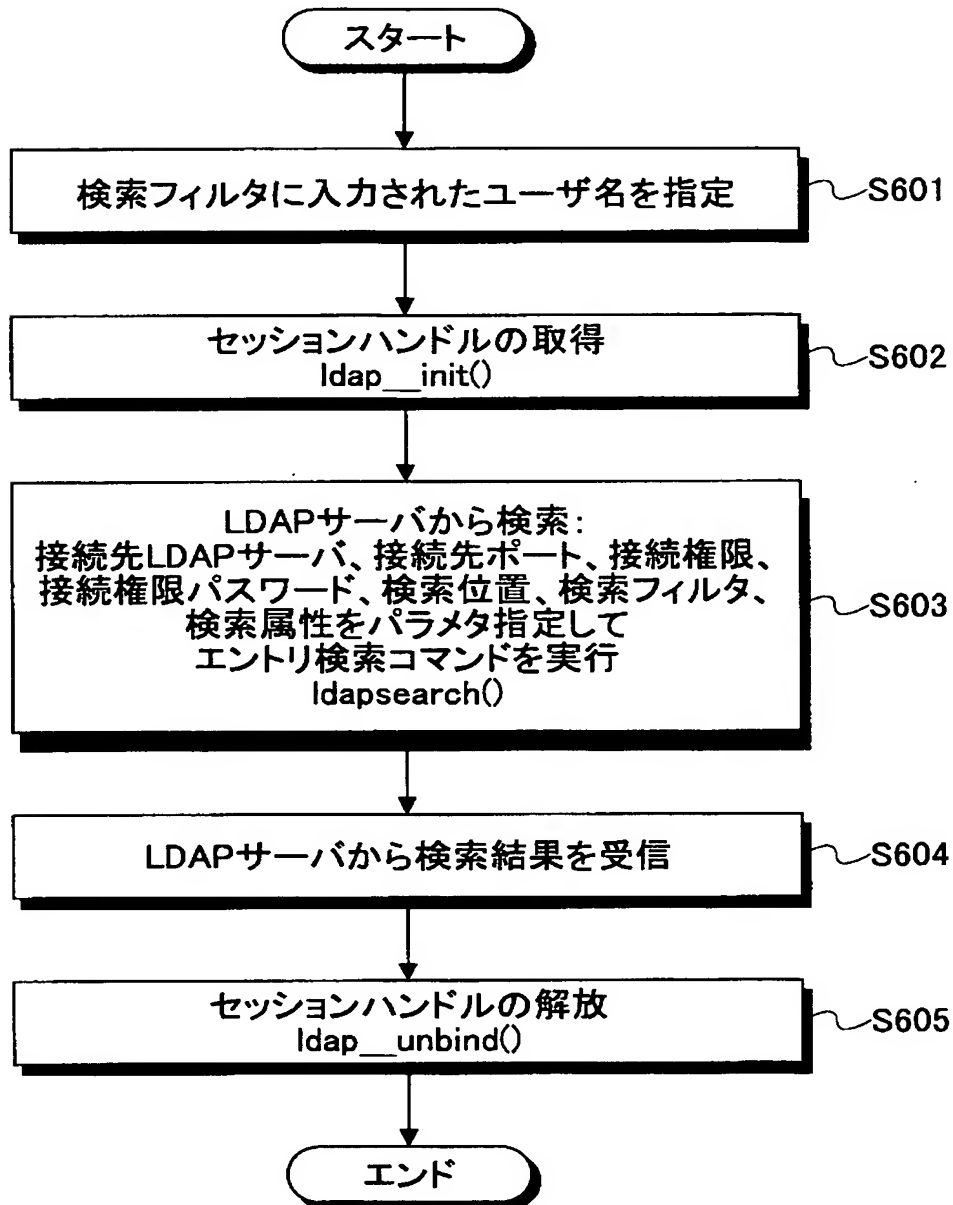
コピー

スキャナ

ファクシミリ

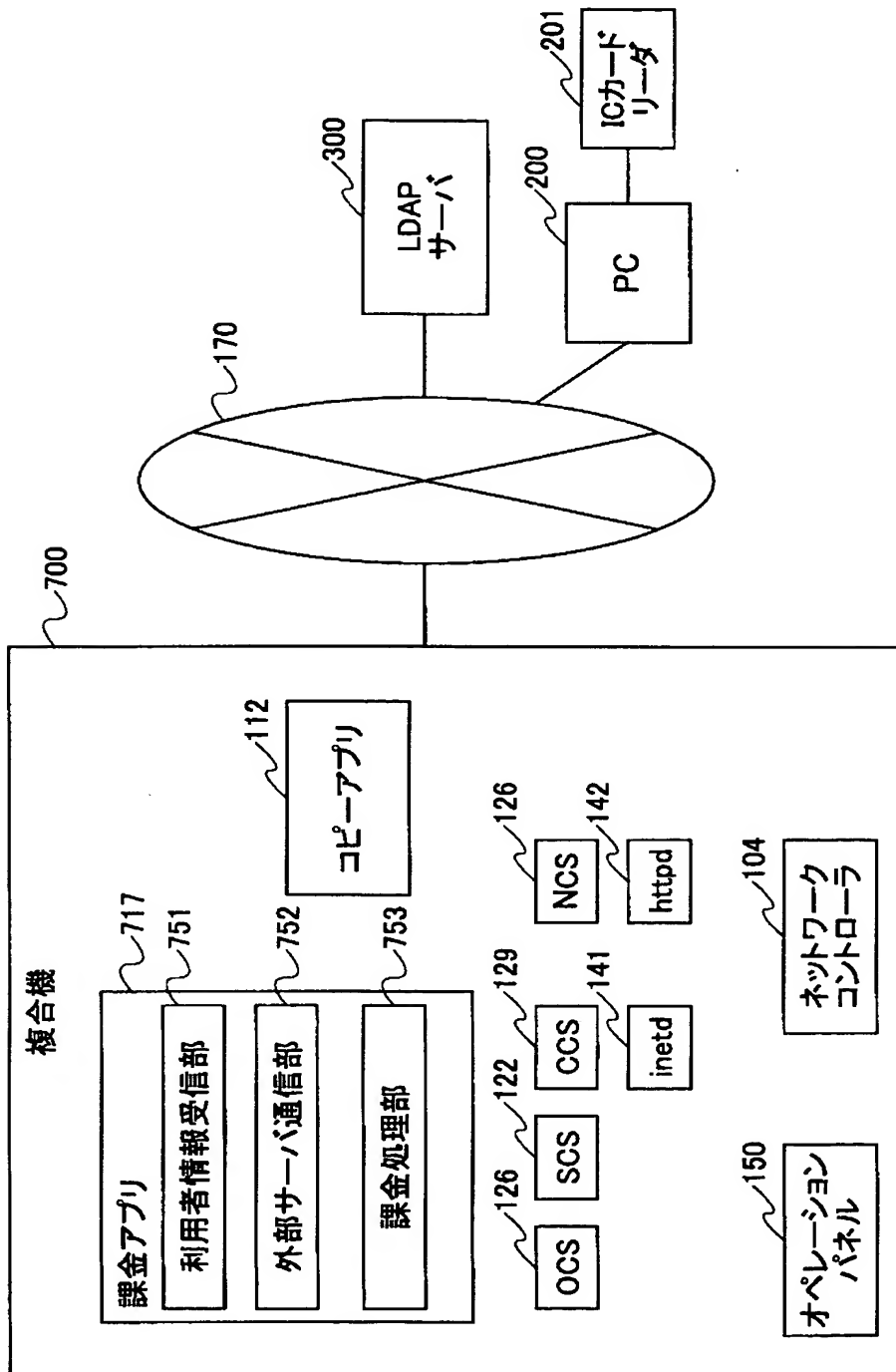
【図 7】

エントリ検索要求処理の手順を示すフローチャート



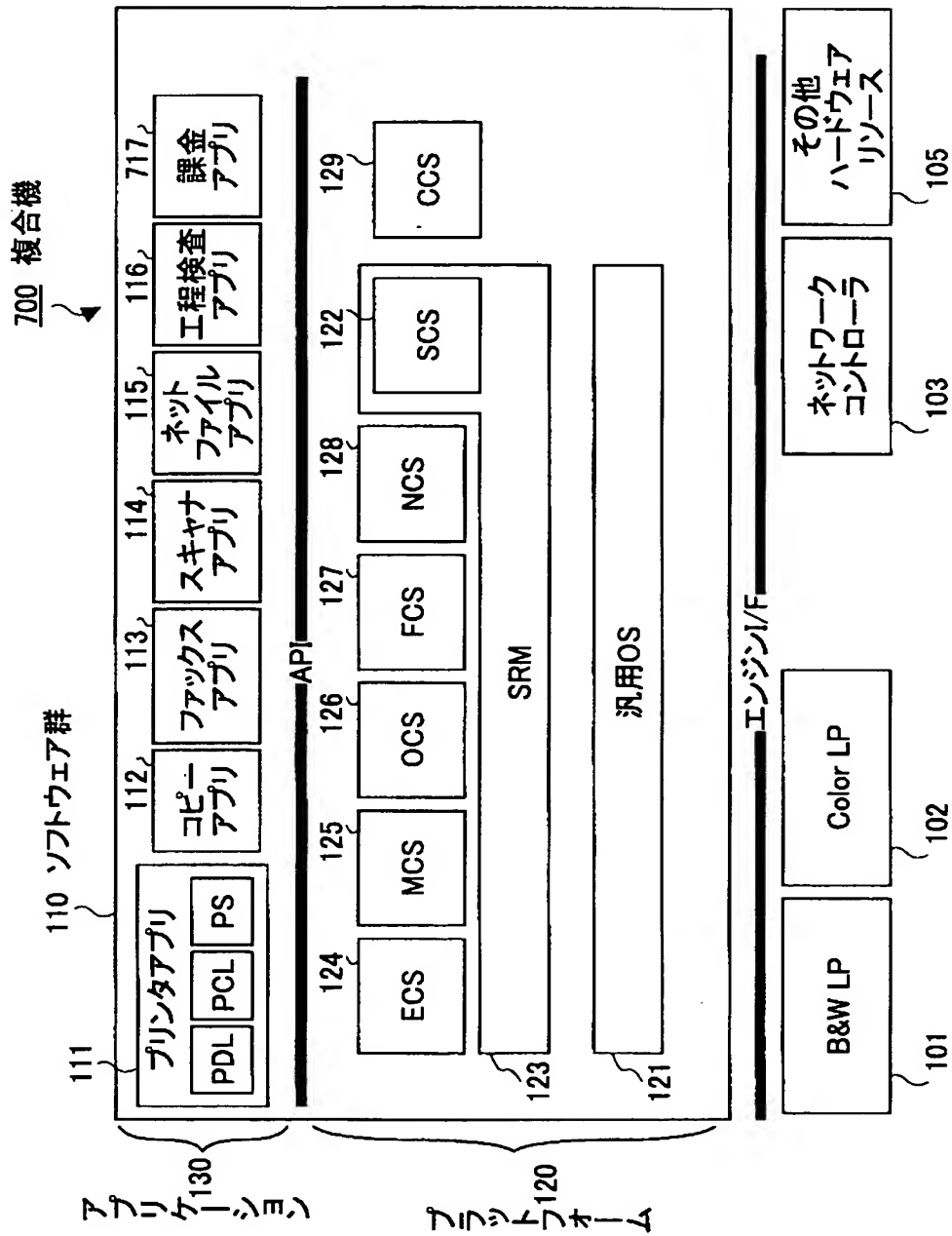
【図 8】

実施の形態2にかかる複合機の主要構成および
複合機を含むネットワーク構成を示す説明図



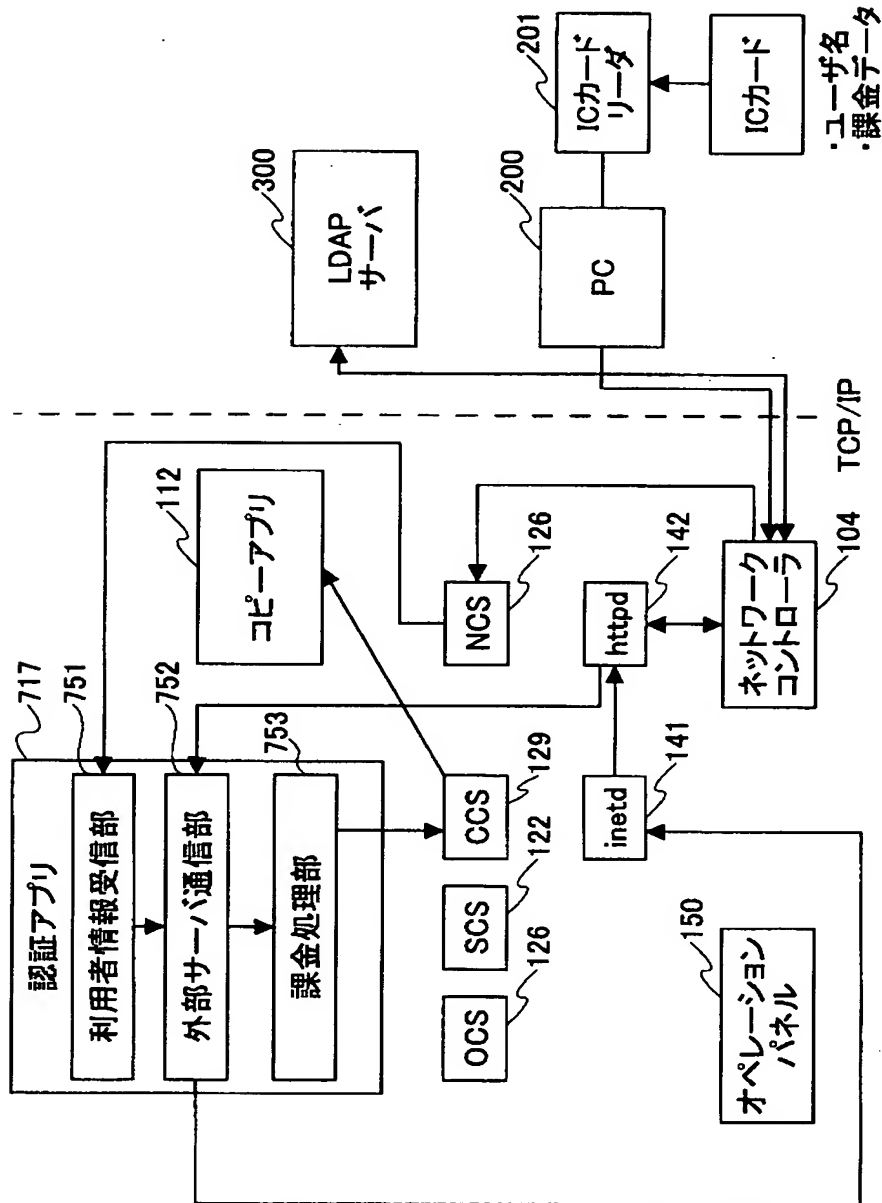
【図 9】

実施の形態2の複合機の全体の機能的構成を示すブロック図



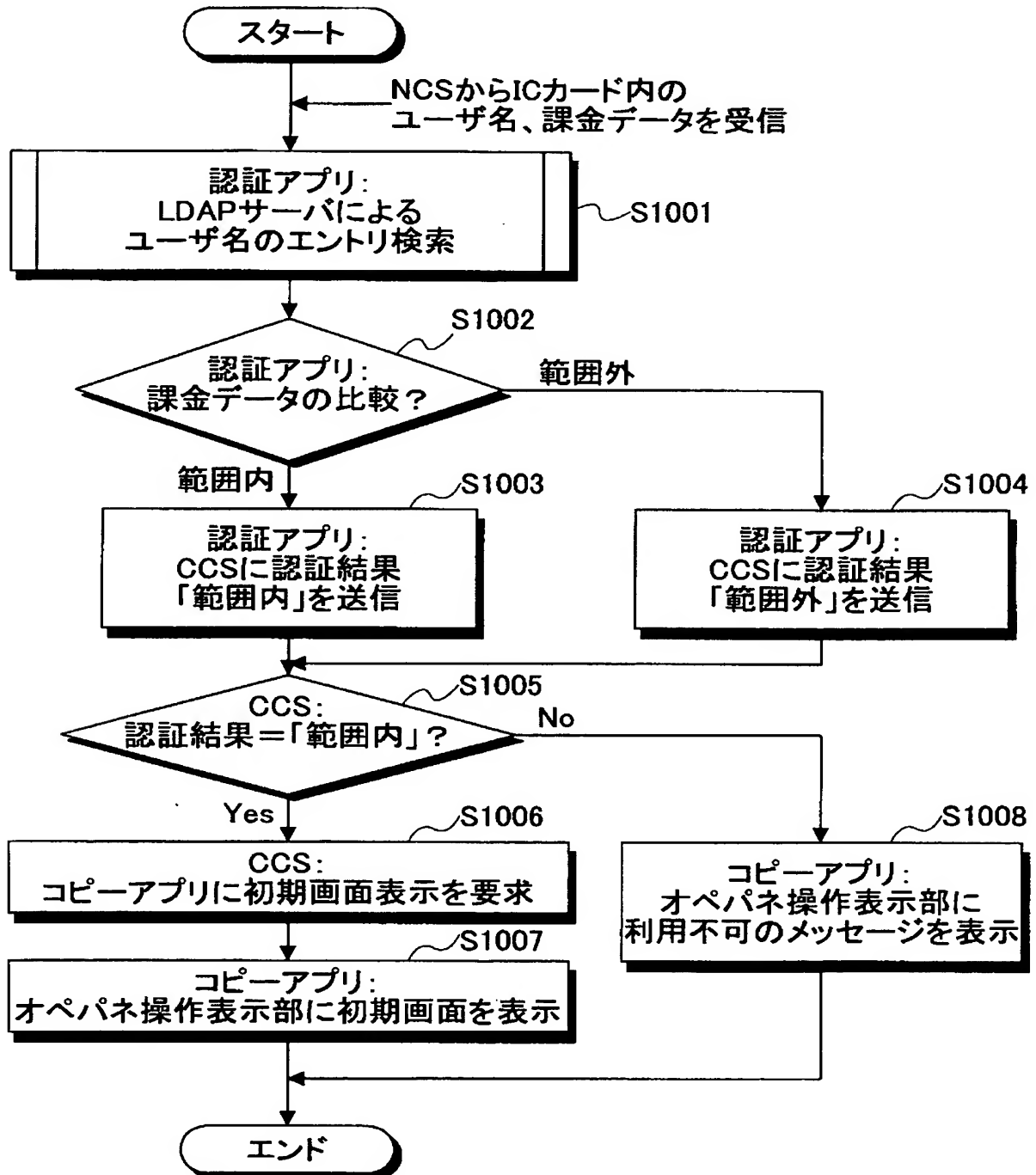
【図 10】

複合機による課金処理および課金に基づく利用制限処理におけるデータの流れを示す説明図



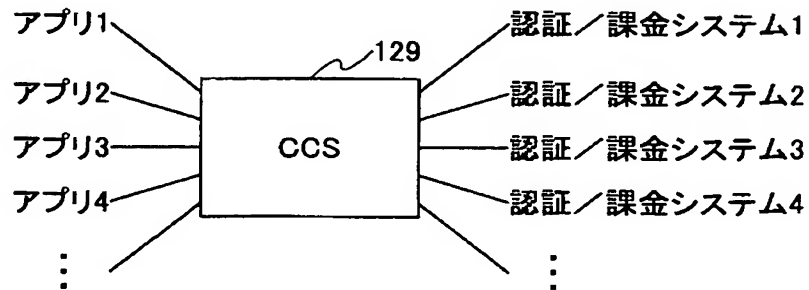
【図 11】

課金処理および課金に基づく利用制限処理の手順を示すフローチャート



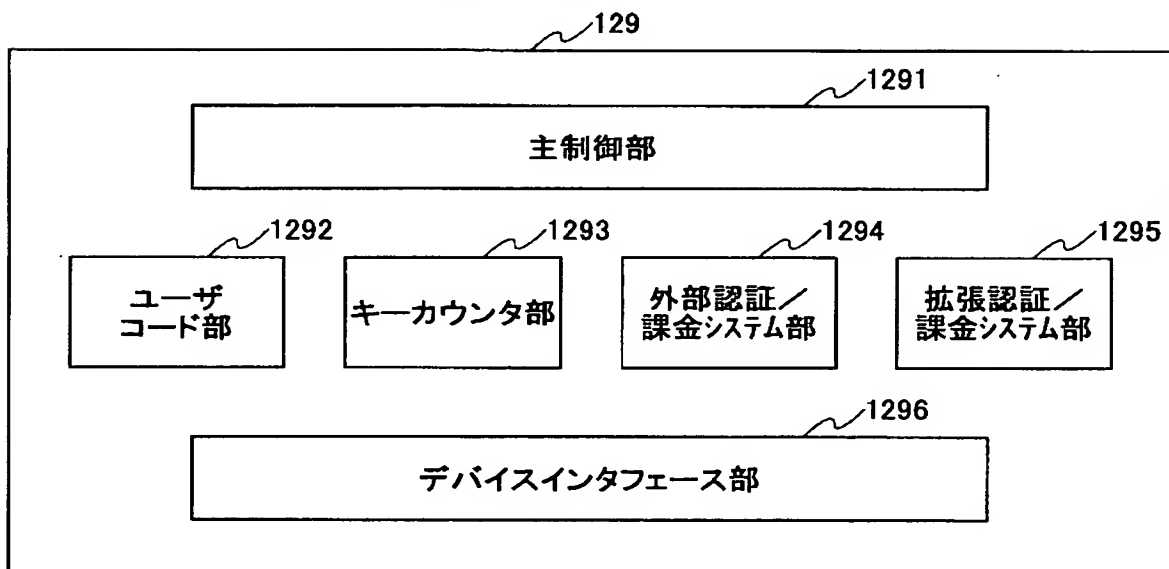
【図 12】

実施の形態3におけるCCSの機能を説明するための図



【図 13】

CCSの機能的構成例を示す図



【図 1 4】

デバイスインタフェース部による処理の一例を説明するための図

```
int key_data(128);
int key_count_read(){
    while (1) {
        fd=open("/dev/usb0","r");
        read (fd, buf);
        if(buf[0]!=0){
            bcopy(buf, key_data);
            send_mesg(main_thread, "call_all_apl");
        }
    }
}
```

【図 1 5】

CCSによる設定画面において、
認証／課金システムの一覧表示がなされている画面の例

ユーザコード管理
キーカウンタ管理
外部課金装置管理
拡張認証／課金システム管理

△ 前へ ▽ 次へ

【図 16】

認証／課金の対象とするアプリの機能を選択するための画面

拡張認証／課金システム1 管理する機能を選択し、[設定]を押してください		
コピー:	プリンター:	その他の機能:
<input type="button" value="フルカラー"/>	<input type="button" value="カラー"/>	<input type="button" value="ドキュメントボックス"/>
<input type="button" value="白黒"/>	<input type="button" value="白黒"/>	<input type="button" value="ファックス"/>
<input type="button" value="単色"/>		<input type="button" value="スキャナー"/>
<input type="button" value="2色"/>		
<input type="button" value="前項"/>	<input type="button" value="次項"/>	<input type="button" value="取消"/> <input type="button" value="設定"/>

【図 17】

認証／課金の対象とするアプリの機能を選択するための画面

拡張認証／課金システム1 管理する機能を選択し、[設定]を押してください		
アプリ1	アプリ2	アプリ3
<input type="button" value="フルカラー"/>	<input type="button" value="カラー"/>	<input type="button" value="白黒"/>
<input type="button" value="白黒"/>	<input type="button" value="白黒"/>	
<input type="button" value="単色"/>		
<input type="button" value="2色"/>		
<input type="button" value="前項"/>	<input type="button" value="次項"/>	<input type="button" value="取消"/> <input type="button" value="設定"/>

【図 18】

図16、17の画面を用いた設定により格納される設定情報の例を示す図

拡張認証／課金システム1				
	アプリ1	アプリ2	アプリ3	...
カラー	制限あり	制限あり		.
白黒		制限あり		.
単色		制限あり		.
2色		制限あり		.

【図 19】

設定画面の他の例を示す図

拡張認証／課金システム1 どちらかを選んでください

[アプリの機能を選択し設定する]

[アプリを選択し設定する]

取消

設定

【図 20】

認証／課金の対象とするアプリを選択するための画面

拡張認証／課金システム1 管理するアプリを選択し、[設定]を押してください

コピー	アプリ1
ドキュメントボックス	アプリ2
プリンタ	アプリ3
ファックス	
スキャナー	

【図 21】

図20の画面を用いた設定により格納される設定情報の例を示す図

	制限の対象となるアプリ
認証／課金システム1	コピー, アプリ1
認証／課金システム2	ファックス
認証／課金システム3	アプリ2
⋮	⋮

【図 22】

設定画面の他の例を示す図

アプリを選択してください

コピー	アプリ1
ドキュメントボックス	アプリ2
プリンタ	アプリ3
ファックス	
スキャナー	

取消 設定

【図 23】

アプリに対して適用する認証／課金システムを選択するための図

アプリ1に適用する認証／課金システムを選択してください

認証／課金システム1	AND OR
認証／課金システム2	
認証／課金システム3	
認証／課金システム4	

取消 設定

【書類名】 要約書

【要約】

【課題】 ネットワーク上の外部サーバを利用した認証／課金システムを含む複数の認証／課金システムを複数のアプリに対して使用することを可能とした画像形成装置を提供する。

【解決手段】 複数のアプリケーションを搭載可能に構成された画像形成装置において、一又は複数の認証手段からの認証結果を受信し、受信した認証結果に基づき、一又は複数のアプリケーションの利用制限を制御する利用制御手段を備える。

【選択図】 図 1 2

特願 2 0 0 3 - 3 1 8 4 7 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー